

Sicherheitsanforderung

Load Balancer als Webserver

Deutsche Telekom Gruppe

Version	5.0
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.59	Dokumententyp Sicherheitsanforderung
Version 5.0	Stand 01.07.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2025 - 30.06.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt. Es definiert die Anforderungen an eine sichere Konfiguration von Load Balancern, die als Webserver genutzt werden. Die hier beschriebenen Anforderungen müssen erfüllt werden, um sicherzustellen, dass die Webserver-Funktionalität des Load Balancers nicht ohne weiteres von sachkundigen Angreifern missbraucht werden kann.

Copyright © 2025 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Load Balancer Software	5
3.	Konfiguration des Load Balancers	7
4.	HTTPS	9
5.	Protokollierung	14

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt. Die Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden.

Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

Anmerkung zum Begriff "**Webserver**":

Ein Load Balancer implementiert nicht die volle Funktionalität eines Webserver, sondern im Wesentlichen die eines Reverse HTTP(S)-Proxies. Der Load Balancer kann also nur dann einen Webserver ersetzen, wenn nur die Funktionalität eines Proxies erforderlich ist.

2. Load Balancer Software

Req 1	Software und Hardware des Systems müssen von einem Sicherheitsschwachstellen-Support seitens des Herstellers abgedeckt werden.
-------	--

In einem System dürfen nur Software- und Hardware-Produkte eingesetzt werden, für die ein Sicherheitsschwachstellen-Support durch den Hersteller besteht.

Ein solcher Support muss umfassen, dass der Hersteller

- das Produkt kontinuierlich auf eine Betroffenheit von Sicherheitsschwachstellen beobachtet und analysiert,
- über Art, Schweregrad und Ausnutzbarkeit von im Produkt entdeckten Schwachstellen umgehend informiert
- zeitnah Produktaktualisierungen oder wirksame Workarounds zur Behebung der Schwachstellen bereitstellt.

Der Sicherheitsschwachstellen-Support muss für die gesamte Dauer bestehen, in der das betroffene Produkt im Einsatz verbleibt.

Support-Phasen mit eingeschränktem Leistungsumfang

Viele Hersteller bieten für ihre Produkte als Option einen zeitlich ausgedehnten Support an, welcher über die für den allgemeinen Markt vorgesehene Support-Phase hinausgeht, aber oftmals mit Einschränkungen verbunden ist. Einige Hersteller definieren ihren Support grundlegend in Abstufungen, die Einschränkungen schon während der letzten Phase vor dem absoluten Endtermin des regulären Supports enthalten können.

Wird ein Produkt innerhalb von Support-Phasen eingesetzt, die Einschränkungen unterliegen, muss explizit sichergestellt werden, dass diese Einschränkungen die Verfügbarkeit des Sicherheitsschwachstellen-Support nicht beeinträchtigen.

Open Source Software und Hardware

Open Source Produkte werden häufig von freien Organisationen oder Communities entwickelt; entsprechend ist ein vertraglich vereinbarter Sicherheitsschwachstellen-Support unter Umständen nicht verfügbar. Grundsätzlich muss auch hier sichergestellt werden, dass von der Organisation/Community (oder einem offiziell durch diese eingesetzten Dritten) für das betroffene Produkt ein umfassendes Sicherheitsschwachstellen-Management betrieben wird, welches die oben genannten Kriterien erfüllt und als zuverlässig etabliert gilt.

Motivation: Hardware- und Software-Produkte, für die kein vollumfassender Sicherheitsschwachstellen-Support durch den Hersteller besteht, stellen ein Risiko dar. Dies bedeutet, dass ein Produkt nicht ausreichend auf eine Betroffenheit durch weiterentwickelte Angriffsformen oder neu entdeckte Schwächen technischer Umsetzungen geprüft wird. Analog werden bei vorhandenen Sicherheitsschwachstellen in einem Produkt keine Nachbesserungen (z. B. Updates, Patches) bereitgestellt. Hieraus resultiert ein System, dessen Schwachstellen nicht behoben werden können, so dass sie für einen Angreifer ausnutzbar bleiben, um das System zu kompromittieren oder es negativ zu beeinträchtigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-1/9.0

Req 2	Bekannte Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden.
-------	--

Bekannte Schwachstellen in Software- und Hardware Komponenten müssen mittels Installation von verfügbaren Systemaktualisierungen des Herstellers (z. B. Patches, Updates/Upgrades) behoben werden. Alternativ ist der Einsatz von Workarounds (Akut-Lösungen, welche die Schwachstelle nicht beheben, aber die Ausnutzung wirksam verhindern) zulässig. Workarounds sollten grundlegend nur temporär Verwendung finden und sobald möglich durch eine re-

guläre Systemaktualisierung ersetzt werden, um die Schwachstellen vollständig zu schließen.

Komponenten, die bekannte, nicht behebbare Schwachstellen enthalten, dürfen in einem System nicht eingesetzt werden.

Die Behandlung von neu bekannt werdenden Schwachstellen muss zudem für die gesamte Einsatzphase des Systems fortlaufend sichergestellt und in den kontinuierlichen Betriebsprozessen eines Security Patch Managements umgesetzt werden.

Motivation: Der Einsatz von Komponenten ohne eine Behebung enthaltener Schwachstellen erhöht deutlich das Risiko einer erfolgreichen Kompromittierung. Der Angreifer wird zusätzlich dadurch begünstigt, dass i. d. R. nicht nur detaillierte Informationen zu bereits bekannt gewordenen Schwachstellen offen verfügbar sind, sondern oft auch bereits angepasste Angriffswerkzeuge, die eine aktive Ausnutzung erleichtern.

Umsetzungsbeispiel: Im Anschluss an die initiale Installation eines Betriebssystems von einem offiziellen Installationsmedium werden alle aktuell verfügbaren Patches und Sicherheits-Updates eingespielt.

Zusätzliche Informationen:

Primäre Quellen für bereits bekannt gewordene Schwachstellen in einer Software/Hardware sind Auflistungen in den Versionshinweisen sowie die Sicherheitshinweise aus den offiziellen Meldekanälen des Herstellers oder unabhängiger CERTs. Insbesondere die Meldekanäle werden sinnvollerweise fest in kontinuierliche Prozesse des Security Patch Managements für ein System eingebunden, damit neu bekanntwerdende Schwachstellen zeitnah registriert und in operative Behebungsmaßnahmen geführt werden können.

Als ergänzende Maßnahme zur Aufdeckung von potenziell noch enthaltenen, grundsätzlich bereits bekannt gewordenen Arten von Schwachstellen können gezielte Schwachstellenuntersuchungen des Systems durchgeführt werden. Zu diesem Zweck eignen sich besonders spezialisierte Werkzeuge wie automatisierte Schwachstellen-Scanner. Beispiele hierfür sind: Tenable Nessus, Qualys Scanner Appliance.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-10/9.0

3. Konfiguration des Load Balancers

Req 3	Der Webserver-Dienst darf nur an die Schnittstellen gebunden werden, über die er erreichbar sein muss.
-------	--

In den meisten Fällen muss der Webserver-Dienst nur an eine Schnittstelle gebunden werden.

Motivation: Je mehr Schnittstellen Zugriff zum Webserver erlauben, desto höher ist ein Angriffsrisiko.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.03-5/8.0

Req 4	Falls der Load Balancer eine HTTP-Konformitätsprüfung unterstützt, muss er HTTP-Anfragen, die nicht den entsprechenden Protokoll-Spezifikationen genügen, ablehnen.
-------	---

HTTP-Anfragen müssen RFC2616 entsprechen. Eine HTTP-Anfrage, die beispielsweise einen inkorrekten Content-Length-Header enthält, muss mit dem passenden HTTP Status-Code abgelehnt werden.

Viele Load Balancer unterstützen eine HTTP-Konformitätsprüfung, z. B. durch "Strict HTTP inspection".

Motivation: Wenn ein Request nicht der Spezifikation gemäß RFC genügt, ist dies möglicherweise ein Hinweis auf einen Angriffsversuch.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.59-4/5.0

Req 5	Nicht benötigte HTTP-Methoden müssen deaktiviert werden.
-------	--

Die TRACE/TRACK-Methode darf bei einem produktiven Webserver nicht verwendet werden. Standard-Requests an Webserver verwenden nur GET und POST. Werden andere Methoden benötigt, müssen diese sicher verarbeitet werden.

Motivation: HTTP TRACE könnte von einem Angreifer missbraucht werden. Diese Methode ermöglicht das Debugging und die Trace-Analyse für Verbindungen vom Client zum Webserver. Andere HTTP-Methoden könnten auch verwendet werden, um Informationen über den Server zu erhalten oder könnten direkt von einem Angreifer missbraucht werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.03-6/8.0

Req 6	Der Server-String im HTTP-Header muss ersetzt werden.
-------	---

Der HTTP-Header darf keine Information zur Version des Load Balancers und verwendeter Module/Erweiterungen enthalten.

Motivation: Jede Information über verwendete Software kann über Sicherheitsschwachstellen Aufschluss geben. Wenn z. B. der Serverstring "Server: Apache/2.4.1 (Unix)" lautet, dann kann ein Angreifer gezielt Schwachstellen dieser Version suchen.

Umsetzungsbeispiel: Ändern der Konfiguration, sodass als HTTP-Header
Server: Webserver
ausgegeben wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.59-6/5.0

Req 7 Lange Laufzeiten von HTTP-Anfragen müssen verhindert werden.

Die Konfiguration von Timeouts, die die Reaktion auf HTTP-Anfragen regeln, muss so erfolgen, dass lange Laufzeiten verhindert werden. Eine Anfrage an den Webserver benötigt im Allgemeinen weniger als 10 Sekunden. Die Möglichkeiten hierzu können je nach Load Balancer-Produkt unterschiedlich sein.

Motivation: Die Performance des Load Balancers kann durch lange Laufzeiten bei HTTP-Anfragen erheblich sinken - bis zu einem Denial-of-Service. Dies kann für einen Angriff ausgenutzt werden (Beispiel: Slowloris).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.59-7/5.0

Req 8 Der Load Balancer muss sich und nachgelagerte Systeme vor Angriffen und fehlerhaften Anfragen schützen.

Load Balancer bieten verschiedene Konfigurationsmöglichkeiten für Schutzmechanismen, z. B.

- Beschränkung der Länge von HTTP-Requests
- Aktivieren von "Slow Start"
- Setzen von "Maximum Connections pro Real Server"
- Schutz von SynFlood

Welche Maßnahmen im Detail konfiguriert werden, hängt von den Möglichkeiten des Load Balancers (siehe die Hersteller-Dokumentation) und den Anforderungen der Applikation auf dem nachgelagerten System ab.

Motivation: Angriffe und fehlerhafte Anfragen sollen an der frühest möglichen Stelle erkannt und abgewehrt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.59-8/5.0

4. HTTPS

Req 9	Für die Verschlüsselung mit HTTPS muss das TLS-Protokoll in Version 1.2 oder höher verwendet werden.
-------	--

SSL und TLS 1.0/1.1 sind als veraltet anzusehen und dürfen daher nicht aktiviert werden bzw. müssen deaktiviert werden. TLS in der Version 1.2 besitzt eine ausreichende Designsicherheit und bietet ebenfalls Cipher mit Authenticated Encryption Associated Data (AEAD)

Motivation: Die aktuellen Versionen von TLS schließen bisherige Sicherheitsschwachstellen und Angriffsflächen auf den TLS Protokoll-Handshake

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.03-21/8.0

Req 10	Der Webserver muss so konfiguriert werden, dass die Nutzung der aktuellen Version des TLS-Protokolls möglich ist.
--------	---

Motivation: Die aktuelle Version des Protokolls bietet den höchsten Schutz und enthält Behebungen von Schwachstellen älterer Versionen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.03-22/8.0

Req 11	Die TLS-Konfiguration muss sichere Cipher-Suites, die Perfect Forward Secrecy (PFS) sicher stellen, verwenden.
--------	--

Cipher Suites spezifizieren die kryptographischen Verfahren einer TLS-Verbindung.

Perfect Forward Secrecy (kurz PFS, auch Forward Secrecy) bedeutet, dass Verbindungsinhalte auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden können.

In TLS v1.2 werden Cipher Suites wie folgt definiert: TLS_AKE_WITH_Enc_Hash.

Nachfolgend wird die Bedeutung der einzelnen Bestandteile erläutert:

- AKE (Authenticated Key Exchange): Authentisiertes Schlüsseleinigungsverfahren für das Handshake-Protokoll
- Enc (Encryption): Verschlüsselungsverfahren mit Betriebsart für das Record-Protokoll
- Hash: Hashfunktion für einen HMAC zur Schlüsselableitung. Sofern Enc kein AEAD-Verschlüsselungsverfahren ist, wird der HMAC außerdem zur Integritätssicherung verwendet.

Die nachfolgende Tabelle listet die zulässigen Cipher Suites mit PFS in TLS v1.2 sowie die Referenzspezifikationen auf. Dabei wurde der Designphilosophie von TLS v1.3 gefolgt, weshalb in dieser Tabelle lediglich AEAD-Konstruktionen aufgelistet sind.

Cipher Suite	IANA-Nr.	Referenzspezifikation
--------------	----------	-----------------------

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0,0x2B	[RFC-5289]
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC0,0x2C	[RFC-5289]
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0,0xAC	[RFC-7251]
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0,0xAD	[RFC-7251]
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC0,0x2F	[RFC-5289]
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x30	[RFC-5289]
TLS_ECDHE_ECDSA_WITH_CHACHA20POLY1305_SHA256	0xCC,0xA9	[RFC-7905]
TLS_ECDHE_RSA_WITH_CHACHA20POLY1305_SHA256	0xCC,0xA8	[RFC-7905]

Die folgenden Cipher Suites mit PFS in TLS v1.2 mit AES-CBC (CBC-Modus) und / oder DHE Cipher Suites sind nur in Bestandsystemen erlaubt:

Cipher Suite	IANA-Nr.	Referenzspezifikation	Hinweis
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC0,0x23	[RFC-5289]	CBC
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC0,0x24	[RFC-5289]	CBC
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xC0,0x27	[RFC-5289]	CBC
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xC0,0x28	[RFC-5289]	CBC
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00,0xA2	[RFC-5288]	DHE
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00,0xA3	[RFC-5288]	DHE
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9E	[RFC-5288]	DHE
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9F	[RFC-5288]	DHE
TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x9E	[RFC-6655]	DHE

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x9F	[RFC-6655]	DHE
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAA	[RFC-7905]	DHE
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x00,0x40	[RFC-5246]	CBC / DHE
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x00,0x6A	[RFC-5246]	CBC / DHE
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x00,0x67	[RFC-5246]	CBC / DHE
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x00,0x6B	[RFC-5246]	CBC / DHE

Hinweis zu DHE Cipher Suites:

Für das authentifizierte Schlüsseleinigungsverfahren (AKE) werden Verfahren basierend auf elliptischen Kurven (ECDHE_ECDSA) bevorzugt. DHE (diskreter Logarithmus) Schlüsselvereinbarungen sind anfälliger gegen DoS (DHeater) Angriffe als ECDHE (elliptische Kurven). Sie werden voraussichtlich vom IETF abgekündigt und vom BSI [TR-02102-2] nur bis zum Jahr 2029 empfohlen.

Hinweis zu Cipher Suites mit AES-CBC:

Cipher Suites mit AES-CBC sind nur mit der TLS-Erweiterung "Encrypt-then-MAC" vom BSI empfohlen ([TR-02102-2]). Die Erweiterung ist aber in den meisten Implementierungen nicht aktivierbar bzw. eine Überprüfung, ob sie aktiv ist, ist nicht möglich.

In TLS v1.3 werden Cipher Suites wie folgt definiert: TLS_AEAD_Hash.

Nachfolgend wird die Bedeutung der einzelnen Bestandteile erläutert:

- AEAD: Authentisiertes Verschlüsselungsverfahren für das Record-Protokoll
- Hash: Hashfunktion für HMAC und HKDF im Handshake-Protokoll

Die nachfolgende Tabelle listet die empfohlenen Cipher Suites mit PFS in TLS v1.3 sowie die Referenzspezifikationen auf.

Cipher Suite	IANA-Nr.	Referenzspezifikation
TLS_AES_128_GCM_SHA256	0x13,0x01	[RFC-8446]
TLS_AES_256_GCM_SHA384	0x13,0x02	[RFC-8446]
TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	[RFC-8446]
TLS_AES_128_CCM_SHA256	0x13,0x04	[RFC-8446]

Hinweis zu CHACHA20 Cipher Suites:

CHACHA20 Cipher Suites: werden nicht (explizit) vom BSI empfohlen, aber bisher sind keine Schwachstellen bekannt, so dass sie als sicher einzustufen sind.

Alle zukünftig spezifizierten Cipher Suites, die den in diesem Dokument definierten Anforderungen entsprechen, können ebenfalls verwendet werden. Dies gilt beispielsweise für Cipher Suites, die eine Hash-Funktion aus der SHA-3-Familie verwenden.

Motivation: Als unsicher erkannte Cipher-Suites bieten keinen ausreichenden Schutz.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.03-23/8.0

Req 12	Die TLS-Konfiguration muss vorsehen, dass beim Verbindungsaufbau die als am sichersten einzustufenden Cipher-Suites mit oberster Priorität ausgewählt werden.
--------	---

Eine Cipher Suite enthält die Definition von vier Algorithmen, die für Schlüsselaustausch, Authentifizierung, Verschlüsselung und als Hash-Funktion verwendet werden. Generelle Richtlinien für die Priorisierung von Cipher-Suites sind:

- Für den Schlüsselaustausch muss das Diffie–Hellman-Verfahren verwendet werden, da dieses Perfect Forward Secrecy bietet. Cipher-Suites mit dem Diffie-Hellman-Verfahren sind an den Zeichenketten DHE oder ECDHE erkennbar. ECDHE hat höhere Priorität als DHE.
- Für die Verschlüsselung ist der Advanced Encryption Standard (AES) mit einer möglichst großen Schlüssellänge zu verwenden.
- Als Hashfunktion ist SHA-2 oder SHA-3 zu verwenden. Sie sind üblicherweise an der Zeichenkette SHA oder SHA-3 mit **angehängter Zahl** (256, 384 oder 512) erkennbar. Achtung: die Zeichenkette SHA ohne Zahl kennzeichnet die Funktion SHA-1, die erheblich weniger sicher ist.

Motivation: Beim Aufbau einer TLS-Verbindung wird auf Basis der sowohl auf Client-Seite als auch auf Server-Seite zur Verfügung stehenden Cipher-Suites eine zu verwendende Cipher-Suite ausgewählt. Um eine möglichst hohe Kompatibilität zu verschiedenen Client-Systemen sicherzustellen können auf Server-Seite nicht nur die aus Sicherheitssicht besten Cipher-Suites angeboten werden. Damit für jeden Client aus den verfügbaren Cipher-Suites dennoch die beste ausgewählt wird und dadurch die Verbindung am besten geschützt wird ist eine entsprechende Priorisierung in der Konfiguration erforderlich.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.03-24/8.0

Req 13	Zertifikate müssen von einer Zertifizierungsstelle ausgestellt werden, deren Zertifikate von den gängigen Webbrowsern erkannt werden.
--------	---

Für kritische Anwendungen, die aus dem Internet nutzbar sind, wird empfohlen, dass ein Extended-Validation-Zertifikat (EV-Zertifikat) verwendet wird.

Motivation: Nur wenn die Zertifizierungsstelle (Certificate Authority, CA) in der CA-Liste des verwendeten Browsers enthalten ist, kann der Browser die Authentizität eines Servers bzw. einer Web-Anwendung überprüfen. Die Ausgabe von EV-Zertifikaten ist an strengere Vergabekriterien gebunden. Wird ein EV-Zertifikat verwendet, wird dies im Browser visualisiert. Auch wenn durch EV-Zertifikate an sich kein Gewinn an Sicherheit erzielt wird, erhöht deren Verwendung die Vertrauenswürdigkeit des Servers beim Nutzer.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.03-25/8.0

Req 14	Zertifikate müssen spätestens nach 1 Jahr ihre Gültigkeit verlieren.
--------	--

Bei Zertifikaten einer internen CA, insbesondere für Maschinenschnittstellen, darf der Zeitraum auf maximal 3 Jahre

verlängert werden.

Motivation: Die Methoden und Techniken, mit denen kryptographische Verfahren analysiert und gebrochen werden, werden fortlaufend weiterentwickelt. Daher kann die Sicherheit von Zertifikaten nur für einen begrenzten Zeitraum gewährleistet werden. Bei einer ausreichenden Schlüssellänge ist nach allgemeiner Einschätzung die Sicherheit der Zertifikate für die geforderte Gültigkeitsdauer von einem Jahr aber gewährleistet.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.03-26/8.0

Req 15	Zertifikate müssen eine Schlüssellänge von mindestens 3072 Bit bei Verwendung von RSA oder mindestens 256 Bit bei Verwendung von ECC aufweisen.
--------	---

Hinweise zu DSA und RSA Zertifikaten:

Für DSA und RSA dürfen Schlüssellängen kleiner als 3000 Bit nur noch in Bestandssystemen [BSI TR-02102-1] bis zum Ende des Jahres 2025 [2] eingesetzt werden und sollten zum nächstmöglichen Zeitpunkt ersetzt werden. Aufgrund der besseren Performanz, sind elliptische Kurven Zertifikate (EC-DSA) zu bevorzugen (falls technisch unterstützt und realisierbar). RSA-PKCS#1 v1.5 darf nur noch in Bestandssystemen eingesetzt werden und sollte, wenn technisch möglich, zum nächstmöglichen Zeitpunkt ersetzt werden [BSI TR-02102-1].

Quellen:

[BSI TR-02102-1] Bundesamt für Sicherheit in der Informationstechnik: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, TR-02102-1, Version 2022-01, 28.01.2022

Motivation: Um die Sicherheit der Zertifikate über den Gültigkeitszeitraum zu gewährleisten, müssen die kryptographischen Schlüssel eine entsprechende Länge aufweisen. Nach allgemeiner Einschätzung bietet eine Schlüssellänge von 3072 Bit einen ausreichenden Schutz für die nächsten Jahre. Bei ECC-Algorithmen bieten kürzere Schlüssellängen bereits dasselbe Maß an Sicherheit.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.03-27/8.0

5. Protokollierung

Req 16	Für sicherheitsrelevante Protokollierungsdaten, die lokal erfasst werden, müssen geltende Aufbewahrungszeiträume und Löschfristen eingehalten werden.
--------	---

Aus Sicht der IT-Sicherheit wird auf einem System die lokale Erfassung von sicherheitsrelevanten Protokollierungsdaten nicht zwingend gefordert. Da lokal erfasste Protokollierungsdaten bei Systemstörungen beschädigt oder von einem erfolgreichen Angreifer gezielt manipuliert werden können, sind sie für sicherheitstechnische bzw. forensische Analysen nur bedingt belastbar. Entsprechend ist für die IT-Sicherheit relevant, dass Protokollierungsdaten an einen separaten Log Server weitergeleitet werden.

Eine lokale Erfassung kann dennoch erfolgen; beispielsweise falls bei der Erzeugung der Protokollierungsdaten eine lokale Speicherung aufgrund technischer Abläufe zunächst unabdingbar ist oder es begründete betriebliche Interessen gibt, Protokollierungsdaten auch lokal vorzuhalten.

Folgende Grundregelung ist bei einer lokalen Erfassung von Protokollierungsdaten zu berücksichtigen:

- Sicherheitsrelevante Protokollierungsdaten müssen für einen Zeitraum von 90 Tagen aufbewahrt werden.
(Diese Anforderung gilt nur, falls auf dem System keine zusätzliche Weiterleitung an einen separaten Log Server umgesetzt ist und Protokollierungsdaten daher ausschließlich lokal erfasst werden.)
- Nach Ablauf von 90 Tagen muss eine umgehende Löschung von gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen (insbesondere im Zusammenhang mit personenbezogenen Daten) bestehen oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für lokal erfasste sicherheitsrelevante Protokollierungsdaten auf einem beispielhaften TK-System umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung nach spätestens 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-34/9.0

Req 17	Für sicherheitsrelevante Protokollierungsdaten, die an den Log Server weitergeleitet werden, muss die Einhaltung geltender Aufbewahrungszeiträume und Löschfristen sichergestellt werden.
--------	---

Folgende Grundregelung ist zu berücksichtigen:

- sicherheitsrelevante Protokollierungsdaten müssen auf dem Log Server für einen Zeitraum von 90 Tagen aufbewahrt werden.
- nach Ablauf von 90 Tagen muss eine umgehende Löschung der auf dem Log Server gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen bestehen (insbesondere im Zusammenhang mit personenbezogenen Daten) oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Log Server in Verantwortung eines Dritten

Sollte der ausgewählte Log Server nicht innerhalb derselben operativen Verantwortung liegen wie das Quellsystem der Protokollierungsdaten, muss sichergestellt werden, dass dem verantwortlichen Betreiber des Log Servers die gültigen Parameter für die zu empfangenden Protokollierungsdaten bekannt sind und durch diesen im Sinne der hier genannten Regelungen eingehalten werden.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für ausgeleitete sicherheitsrelevante Protokollierungsdaten eines beispielhaften TK-Systems auf dem separaten Log Server umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung spätestens nach 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-36/9.0